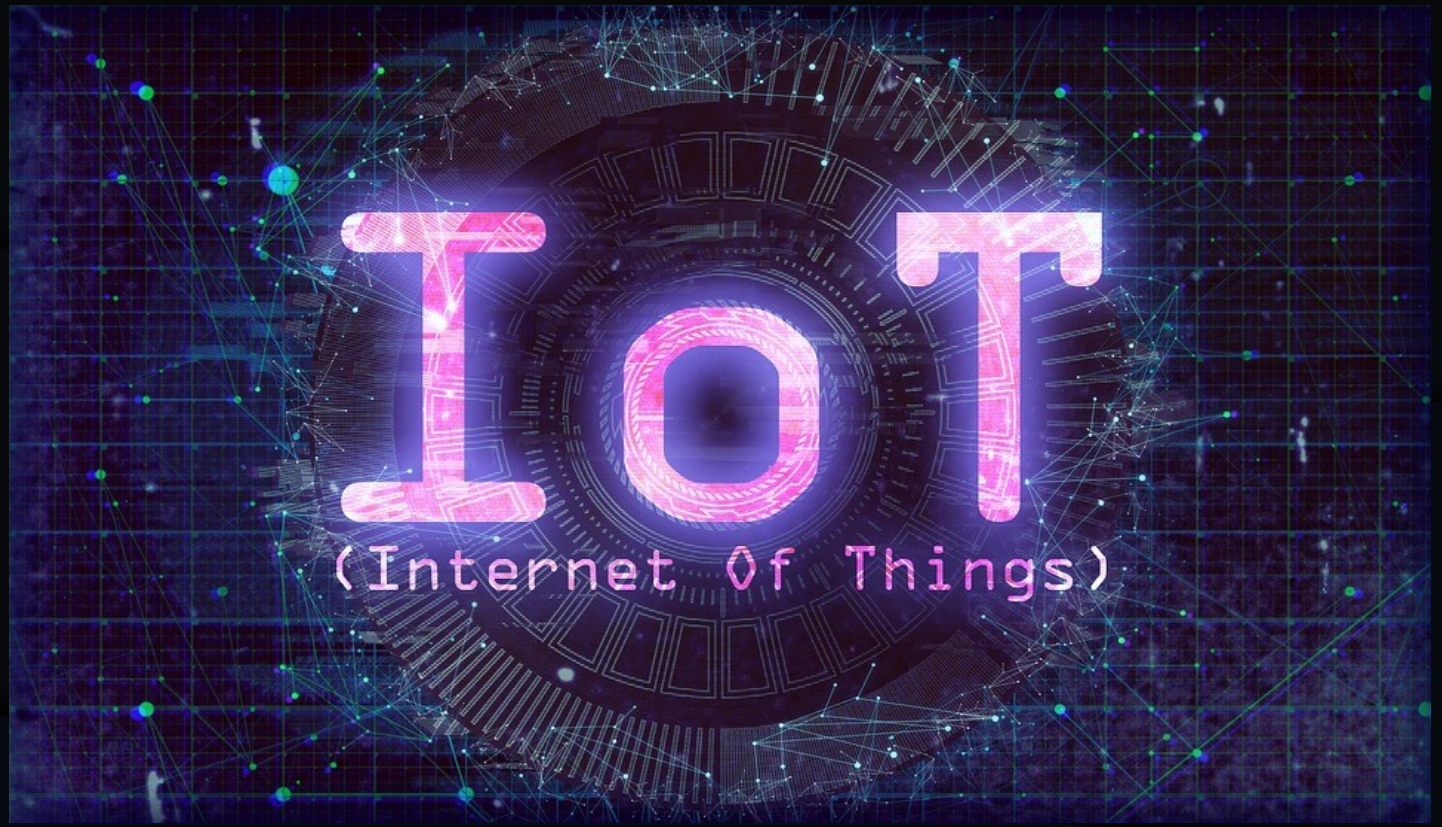


IoT: MQTT en Ecuador

christian leonardo quezada paida

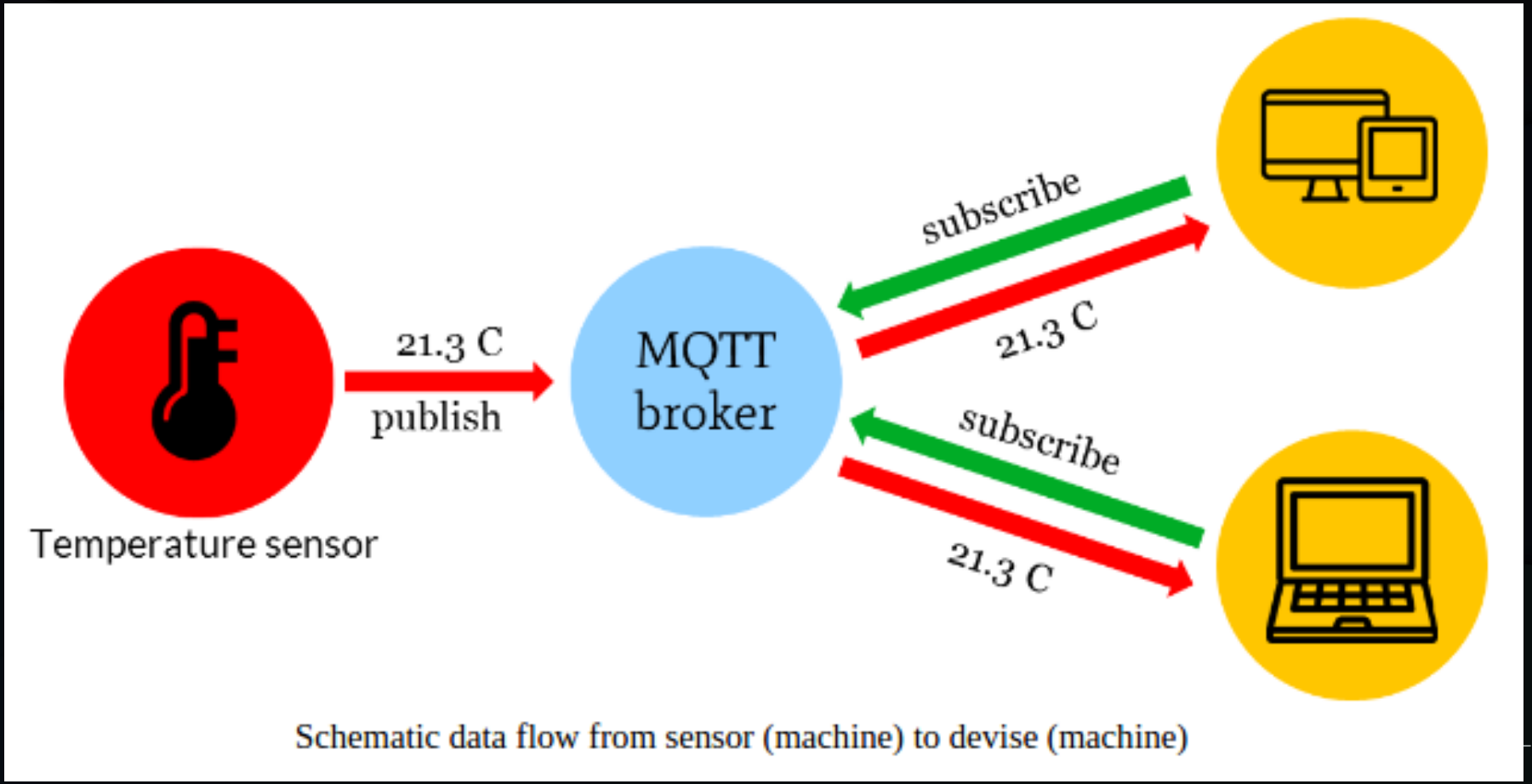
¿Qué es MQTT?

- MQ Telemetry Transport
- Telemetría = Mediciones Remotas
- Protocolo de mensajeria liviano para comunicaciones M2M
- Inventado por IBM, ahora OpenSource

¿Cómo funciona MQTT?

- Usa un mecanismo de mensajeria push del tipo publicador/suscriptor
- Se puede tener un “servidor” llamado BROKER
- Los mensajes se filtran en “topics” organizados jerárquicamente
- Ejm: *temperatura/, casa/segundo_piso/foco1*

Flujo de datos del protocolo



Schematic data flow from sensor (machine) to devise (machine)

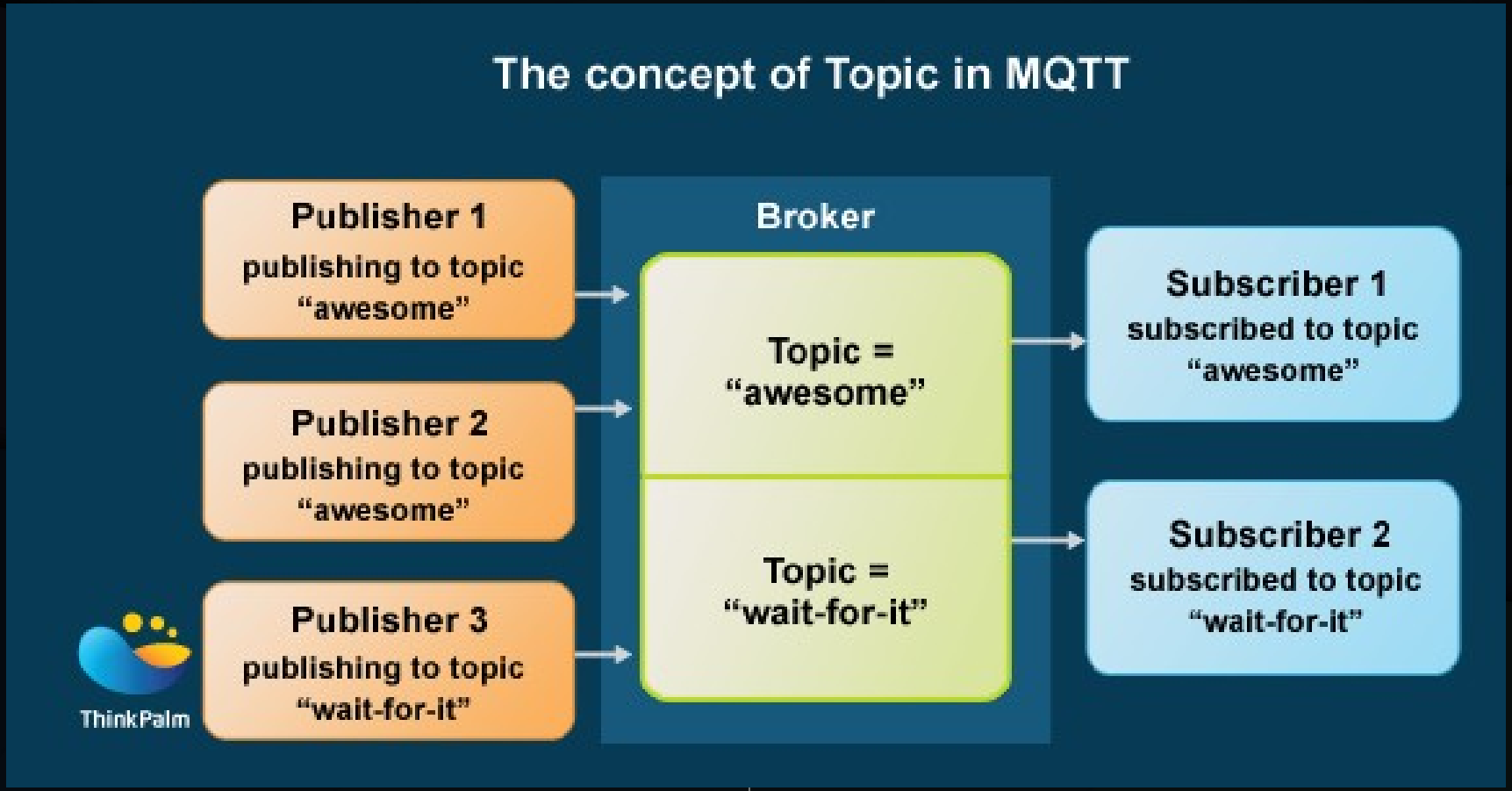
¡Vamos un poco más técnico!

- Puerto por default: 1883 definido por la IANA como MQTT sobre TCP
- Tiene 3 niveles de QoS
  - 0: El mensaje se envía una única vez, si falla no se entregará
  - 1: El mensaje se envía hasta garantizar la entrega, si falla puede recibir más de una vez el mensaje
  - 2: El mensaje garantiza entrega una sola vez al suscriptor

¿Topics MQTT?

- Ejm: *temperatura/, casa/segundo_piso/foco1*
- *Un cliente puede suscribirse a un topic para que el broker les haga llegar los mensajes publicados del topic específico suscrito*

Concepto de Topic en MQTT



¡Vamos un poco más técnico!

- Códigos de respuesta
  - Con. Aceptada: 0
  - Con. Rechazada, versión protocolo inaceptable: 1
  - Con. Rechazada, identificador rechazado: 2
  - Con. Rechazada, servidor inaccesible: 3
  - Con. Rechazada, mal usuario o password: 4
  - Con. Rechazada, no autorizado: 5

¡Volvamos a los Topics!

- Los topics son case-sensitivo
- Wilcard
  - Nivel único: Reemplaza un único nivel con el signo “+”. Ejm: casa/piso1/+/foco_cuarto
  - Multi nivel: Reemplaza multiples niveles con el signo “#”. Ejm: casa/piso1/#

¡Volvamos a los Topics!

- Topics que inician con $
- Tienen el proposito de brindar información sobre el broker, estadísticas internas
- No se pueden publicar a estos topics
- No existe una estandarización oficial pero aqui hay información al respecto https://github.com/mqtt/mqtt.github.io/wiki/SYS-Topics

¡Volvamos a los Topics!

- Algunos topics principales son
  - $SYS/broker/clients/connected, Número de clientes conectados
  - $SYS/broker/clients/disconnected: Número de clientes registrados al broker pero actualmente desconectados
  - $SYS/broker/messages/received: Número Total de mensajes de cualquier tipo recibidos desde que inicio el broker

¡Volvamos a los Topics!

- Algunos topics principales son
  - $SYS/broker/messages/sent: Número total de mensajes de cualquier tipo enviados desde que el broker inició
  - $SYS/broker/uptime: Cantidad de tiempo en segundos que el broker esta online
  - $SYS/broker/version: Versión del Broker

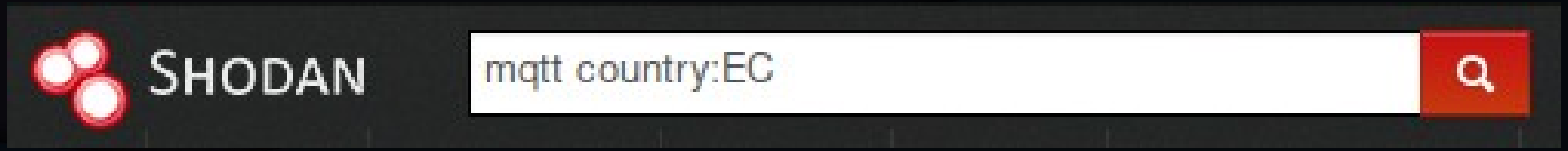
Implementaciones de Broker

- Mosquitto, escrito en C y probablemente el más popular
- Mosca, basado en Node.js
- Emqttd, escrito en Erlang
- Paho, Libreria mqtt para trabajar con Python
- HiveMQ, escrito en Java

¿Y ahora?

¿Y en Ecuador?

La busqueda



El resultado

TOTAL RESULTS

18

TOP COUNTRIES

Ecuador 18

TOP CITIES

Quito 6

Guayaquil 4

Loja 1

Ambato 1

En resumen:

- Total de servidores: 18
  - Código 0 = 12, representan el 66.67%
  - Código 5 = 6, representan el 33.33%
- Tipo:
  - Instituciones Educativas - Código 0: 100%
  - Telco. Privadas – Código 0: 66.7%
  - Telco. Publicas – Código 0: 0%

¿Husmeamos?

- Usando mosquitto
  - apt install mosquitto-clients
  - mosquitto_sub -h **ip_dir** -t "#" -v -q 1 -p **port**
    - h direccion ip
    - v modo verboso
    - q definimos el QoS (opcional)
    - p puerto (opcional)
    - t “#” suscribimos todos los topics

¿Husmeamos?

- Usando script en Python:
  - https://github.com/richiprieto/Charlas_Cursos/blob/master/mqtt_spy.py
  - pip3 install paho-mqtt
  -

```python
import paho.mqtt.client as mqtt

def on_connect(client, userdata, flags, rc):
   print ("[+] Listo")
   client.subscribe('#', qos = 1)        # Suscribimos todos los topicos
   client.subscribe('$SYS/#')            # Estadisticas broker

def on_message(client, userdata, msg):
   print ('[+] Topic: %s - Mensaje: %s' % (msg.topic, msg.payload))

client = mqtt.Client(client_id = "s4p0")
client.on_connect = on_connect
client.on_message = on_message
client.connect('ip_dir', 1883, 60)
client.loop_forever()
```

¿Hackeamos?

¿Hackeamos?

- https://mqtt-pwn.readthedocs.io/en/latest/intro.html
- Fuerza Bruta de Credenciales
- Command & Control
- Conectar al broker
- Recolector de información (Broker $SYS)
- Owntracks (GPS)
- “Sonoff” Exploiter (smart switch para domótica)
- Enumeración (Topics)
- Crear Extensiones

Gracias!

- Twitter: @richiprieto
- Celular: 0988511884